What is claimed is:

1. A device for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and c being a quantity to be subjected to the modular exponentiation, comprising:

means for calculating a first auxiliary quantity dp, wherein dp is defined as follows:

$$dp = d \bmod (p - 1),$$

wherein p is a first prime number;

means for calculating a second auxiliary quantity dq, wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

means for generating a random number (IRND);

means for generating a third auxiliary quantity dp´, wherein dp´ is defined as follows:

$$dp' = IRND \times (p - 1) + dp;$$

means for generating a fourth auxiliary quantity dq´, wherein dq´ is defined as follows:

$$dq' = IRND \times (q - 1) + dq;$$

means for generating a fifth auxiliary quantity Mp, wherein the fifth auxiliary quantity Mp is defined as follows:

$$Mp = c^{dp'} \bmod p;$$

means for generating a sixth auxiliary quantity Mq, wherein the sixth auxiliary quantity Mq is defined as follows:

$$Mq = c^{dq'} \bmod q; \text{ and}$$

means for calculating the result of the modular exponentiation m, wherein m is defined as follows:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

2. The device according to claim 1, further comprising means for generating a safety parameter T,

wherein the means for generating the fifth auxiliary quantity Mp is formed to calculate the fifth auxiliary quantity as follows:

$$Mp = c^{dp'} \bmod (pT), \text{ and}$$

wherein the means for generating the sixth auxiliary quantity Mq is formed to calculate the sixth auxiliary quantity Mq as follows:

$$Mq = c^{dq'} \bmod (q \times T).$$

3. The device according to claim 2, further comprising means for calculating a seventh auxiliary quantity H7, wherein the seventh auxiliary quantity H7 is defined as follows:

$$H7 = Mp \times Mq \bmod T, \text{ and}$$

wherein means for calculating an eighth auxiliary quantity H8 is further provided, wherein the eighth auxiliary quantity H8 is defined as follows:

$$H8 = c^{(dp'+dq')\bmod(T-1)} \bmod T; \text{ and}$$

means for comparing the seventh and eighth auxiliary quantities, wherein the means for comparing is arranged to indicate a fault when the seventh and eighth auxiliary quantities differ.

4. The device according to claim 1, being provided for an RSA decryption or RSA signature, m being a plain text message, d being a secret key and c being an encrypted message.

5. A device for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and c being a quantity to be subjected to the modular exponentiation, comprising:

means for calculating a first auxiliary quantity dp, wherein dp is defined as follows:

$$dp = d \bmod (p - 1),$$

wherein p is a first prime number;

means for calculating a second auxiliary quantity dq, wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

means for providing a safety parameter T;

means for generating a third auxiliary quantity p x T and a fourth auxiliary quantity q x T;

means for generating a fifth auxiliary quantity Mp, wherein the fifth auxiliary quantity Mp is defined as follows:

$$Mp = c^{dq} \bmod (p \times T);$$

means for generating a sixth auxiliary quantity Mq, wherein the sixth auxiliary quantity Mq is defined as follows:

$$Mq = c^{dq} \bmod (q \times T);$$ and

means for calculating the result of the modular exponentiation m, wherein m is defined as follows:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

6. The device according to claim 5, wherein the safety parameter T is a prime number.

7. The device according to claim 3, wherein the safety parameter T is small compared to the first prime number p and the second prime number q, respectively.

8. A method for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and c being a quantity to be subjected to the modular exponentiation, comprising the following steps:

calculating a first auxiliary quantity dp, wherein dp is defined as follows:

$$dp = d \bmod (p - 1),$$

wherein p is a first prime number;

calculating a second auxiliary quantity dq, wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

providing a random number (IRND);

generating a third auxiliary quantity dp´, wherein dp´ is defined as follows:

$$dp' = IRND \times (p - 1) + dp;$$

generating a fourth auxiliary quantity dq´, wherein dq´ is defined as follows:

$$dq' = IRND \times (q - 1) + dq;$$

generating a fifth auxiliary quantity Mp, wherein the fifth auxiliary quantity Mp is defined as follows:

$$Mp = c^{dp'} \bmod p;$$

generating a sixth auxiliary quantity Mq, wherein the sixth auxiliary quantity Mq is defined as follows:

$$Mq = c^{dq'} \bmod q; \text{ and}$$

calculating the result of the modular exponentiation m, wherein m is defined as follows:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$

9. A method for calculating a result of a modular exponentiation, n being a modulus, d being an exponent and c being a quantity to be subjected to the modular exponentiation, comprising the following steps:

calculating a first auxiliary quantity dp, wherein dp is defined as follows:

$$dp = d \bmod (p - 1),$$

wherein p is a prime number;

calculating a second auxiliary quantity dq, wherein dq is defined as follows:

$$dq = d \bmod (q - 1),$$

wherein q is a second prime number,

wherein a product of p and q equals the modulus n;

generating a safety parameter T;

generating a third auxiliary quantity p x T and a fourth auxiliary quantity q x T;

generating a fifth auxiliary quantity Mp, wherein the fifth auxiliary quantity Mp is defined as follows:

$$Mp = c^{dp} \bmod (p \times T);$$

generating a sixth auxiliary quantity Mq, wherein the sixth auxiliary quantity Mq is defined as follows:

$$Mq = c^{dq} \bmod (q \times T);$$ and

calculating the result of the modular exponentiation m, wherein m is defined as follows:

$$m = Mq + [(Mp - Mq) \times q^{-1} \bmod p] \times q.$$